ACCESS METHOD AND DEVICE FOR SECURING ACCESS TO INFORMATION SYSTEMS

[0001] The present invention concerns a method and a device for securing access to information systems.

Definitions

[0002] In the sense of the present invention, the term "applications" generally designates software applications in the communications field.

[0003] In the sense of the present invention, "application" protocol generally designates a protocol that governs the exchange of information between applications.

[0004] In the sense of the present invention, "application" attack designates an attack that uses:

- either the vulnerabilities of an "application" protocol,
- or the vulnerabilities linked to the implementation of an "application" protocol by a developer,
- or the vulnerabilities linked to the use of an application, particularly by a network administrator.

The Problem Posed

[0005] Context: Security of access to information systems

[0006] All experts agree on the fact that the risk linked to computer security is significantly on the rise.

[0007] What are the factors in the growth of this risk?

[0008] Three main factors have been identified.

[0009] First risk factor: the exponential growth in the number of pirates.

[0010] The number of internet users has doubled in three years. They make use of free toolboxes available on the net. International legislation aimed at reducing fraud is nonexistent; for example, in Japan there are no cyber-delinquency laws. Moreover, there is a new type of pirate emerging in high schools and on university campuses, for whom piracy is a game and cracking the largest number of sites is a competition. These computer pirates, commonly known as "script kiddies," have very little technical know-how, but they are able

to use program "toolboxes," generally found on the Internet, that make it possible to attack computer systems.

[0011] Second risk factor: the globalization of trade.

[0012] In the era of cost reduction and the communicating company, companies are obliged to use efficient communication media like the Internet that allow the use of email exchanges, e-commerce sites, and EDI (electronic data interchange).

[0013] Companies are exchanging more and more documents. These documents contain more and more information. This information is of greater and greater value.

[0014] Moreover, companies have to move quickly. They do not always take all the precautions they ought to take.

[0015] Third risk factor: as companies open up worldwide, information systems are also increasingly open to the outside. Information systems are interconnected. A company's LAN (Local Area Network) becomes one of the stations in the global network.

[0016] It is also clear that information systems are becoming more and more complex. Because of this, they have bugs – in other words, holes in their security. In addition, complex information systems are difficult to manage, and consequently, difficult to secure.

[0017] The 2001 CERT (Computer Emergency Response Team) statistics listed, 52,658 incidents in 2001, or an increase of 142% relative to 2000.

[0018] How does one succeed in penetrating a computer system?

[0019] Nearly all vulnerability attacks can be divided into three categories:

[0020] - (a) Attacks that exploit a weakness in the protocols used (for example IP Sniffing). IP Sniffing is a technique that consists of intercepting a communication in a network in order to obtain information.

[0021] - (b) Attacks that exploit a bug found in the TCP/IP stack of the operating system. Certain attacks are known as "Ping of Death" or "Teardrop" attacks.

[0022] Let's briefly review, in the sense of the present invention, the following abbreviations:

- TCP: Transmission Control Protocol; designates a transport protocol (OSI Level 4) used in the TCP/IP family of protocols.

- TCP/IP: Transmission Control Protocol/Internet Protocol; designates a family of protocols used in the interconnection of IP-type networks.

[0023] - (c) "Application" attacks use the transported data. These include, in particular, "application" attacks that exploit bugs in a system's communication applications, for example security holes in the DNS/BIND servers or IIS web servers.

[0024] Let's briefly review, in the sense of the present invention, the following abbreviations:

- DNS (Domain Name System) designates an "application" protocol that allows the system name (for example, www.yahoo.com) to be converted into an IP address (for example (123.234.231.135),
- IP (Internet Protocol) designates a network protocol (OSI Level 3) used on the Internet.

[0025] It is clear from the statistics that the vast majority of the vulnerabilities discovered are on the level of "application" attacks. Thus, the main threat exists at the level of the security holes in communication applications.

[0026] The problem posed by the present invention is to reduce the risks of "application" attacks.

The Prior Art

[0027] There are two known technologies for solving the problem posed and providing IP network security:

[0028] The technology hereinafter referred to as "Stateful" technology.

[0029] The technology hereinafter referred to as "Proxy" technology.

[0030] (a) "Stateful" technology, otherwise known as maintaining an active connection table

[0031] (a1) "Static packet filtering" technology

[0032] The first functionalities for protecting IP networks were integrated into routers. Routers incorporate a static IP packet filtering mechanism. Based on the information read in the header of an IP packet, at the level of the Network and Transport headers, the packet is accepted or rejected in accordance with a list of filtering rules defined by an administrator. The chief drawback of this technology is its static aspect. It cannot attach a

"response packet" to a "request packet" sent a few moments earlier. Consequently, when using a "static packet filtering" technology, one is obliged to accept all the "response packets' without being able to attach them to the requests sent previously. This creates a problem in terms of security since one need only, for example, set the ACK flag in the TCP header of a packet in order for this packet to be accepted by the router. Let's briefly recall that in the sense of the present invention, the abbreviation ACK (ACKnowledgement) designates a flag used in a TCP-type header.

[0033] (a2) "Stateful" technology

[0034] "Stateful" technology partially overcomes this drawback by maintaining an active connection table, which makes it possible to attach the "response packets" to the "request packets" sent previously. In addition, this technology generally involves reading information in the transported data, as opposed to the information contained in the header of the packet, in order to be able to manage secondary connections, based on dynamic ports. For example, any FTP transfer uses a dynamic secondary connection, wherein the ports are negotiated via the control connection in the TCP/21 port. Let's briefly recall that in the sense of the present invention the abbreviation FTP (File Transfer Protocol) designates a protocol used to transfer files in a TCP/IP-type network.

[0035] "Stateful" technology is generally implemented in a system's kernel, or embedded in a real-time system, which ensures good performance in terms of speed. However, "Stateful" technology does not make it possible to ensure conformity with the "application" protocols during a data exchange, since "Stateful" technology is limited to extracting from the transported data the information required to establish and maintain secondary connections. Yet as explained above, the risks of attack exist mainly at the level of the transported data.

[0036] (b) "Proxy" technology

[0037] In the case of "Proxy" technology, otherwise known as "Agent" technology, the client does not address the server directly. For example, the browser, also known as the navigator, connects to the Web server, also called the network server, by going through a "proxy" that performs the request in its place and sends back the response.

[0038] This technology makes it possible to filter the transported data, which is a clear advantage in terms of security. On the other hand, the fact that it is implemented as an

application located "above" the operating system makes it much less efficient in terms of speed than "Stateful" technology. This major drawback of "Proxy" technology results in inadequate performance in terms of the desired speeds in IP networks.

Conclusion

[0039] The drawbacks of the known solutions may be summarized as follows.

[0040] In "Stateful" technology, the security is inadequate.

[0041] In "Proxy" technology, the speed is inadequate.

The Solution According to the Invention

[0042] The technology proposed by the present invention will hereinafter be designated by the abbreviation FAST, for Fast Application Shield Technology. FAST technology solves the problem posed while avoiding the drawbacks of the known "Stateful" and "Proxy" technologies. FAST technology makes it possible to secure access to information systems while avoiding the risk of "application" attacks and limiting the loss of speed.

Method

[0043] The invention concerns a method for securing logical access to information and/or computing resources in a group of computer equipment while slowing down logical access as little as possible. The group of computer equipment exchanges data with a computer telecommunication network, via an access device. The data include transported data that conform to at least one application protocol, as well as transport data. The access device includes an operating system.

[0044] The method according to the invention comprises the following steps:

[0045] - the step of defining, for each application protocol, a finite-state machine,

[0046] - the step of modeling, in the form of a model, each finite-state machine,

[0047] - the step of generating from each model, by means of an interpreter, an analysis module for each application protocol,

[0048] - the step of filtering the transported data in the operating system, by means of the analysis modules.

[0049] Preferably, according to the invention, the method also comprises the step of verifying, by means of the analysis modules, the conformity of the transported data with the application protocols involved.

[0050] Preferably, according to the invention, the method also comprises the step of restricting, by means of the analysis module, the capabilities offered by an application protocol.

[0051] As a result of the combination of these two functionalities (Verify and Restrict), the technology according to the invention makes it possible to detect and block a large number of "application" attacks. These two functionalities have been shown to detect and block 90% of the known attacks on Apache and IIS Web servers without its being necessary to integrate an "attack signature base" into them, as in the case of intrusion detection systems.

[0052] Preferably, according to the invention, the method also comprises the step, for a network administrator, of parameterizing the analysis modules in accordance with predetermined restrictions.

Device

[0053] The invention also concerns an access device for securing logical access to information and/or computing resources in a group of computer equipment while slowing down logical access as little as possible. The group of computer equipment exchanges data with a computer telecommunication network, via the access device. The data include transported data that conform to at least one application protocol, as well as transport data. The access device includes:

[0054] - an operating system that includes an appropriate analysis module for each application protocol,

[0055] - filtering means for filtering the transported data in the operating system, by means of the analysis modules.

[0056] Preferably, according to the invention, each analysis module implements a finite-state machine representing a given application protocol.

[0057] Preferably, according to the invention, the analysis modules include first information processing means for verifying the conformity of the transported data with the application protocols involved.

[0058] Preferably, according to the invention, the analysis modules include second information processing means for restricting the capabilities offered by an application protocol.

[0059] Preferably, according to the invention, the access device also comprises parameterization means that allow a network administrator to parameterize the analysis modules in accordance with predetermined restrictions.

Detailed Description

[0060] Other characteristics and advantages of the invention will emerge through the reading of the description of variants of embodiment of the invention given as illustrative and nonlimiting examples, and from:

[0061] - Fig. 1, which schematically represents a local area network 3 protected by a device 6 according to the invention against attacks originating from an Internet-type computer communication network,

[0062] - Fig. 2, which represents the structure of the data 4 exchanged via a device 6 according to the invention,

[0063] - Fig. 3, which schematically represents a device 6 according to the invention,

[0064] - Fig. 4, which schematically represents the method for constructing an analysis module 14 from a finite state machine.

[0065] Referring to the figures, and particularly Fig. 1, we will now describe a local area network 3 protected by a device 6 according to the invention against attacks originating from an Internet-type computer communication network 5.

[0066] The purpose of the access device 6 is to secure logical access to information 1 and/or computing resources 2 in a group of computer equipment 3 while slowing down said logical access as little as possible.

[0067] The group of computer equipment 3 exchanges data 4 with a computer telecommunication network 5, via said access device 6. In the case of the variant of

embodiment described, the computer telecommunication network 5 is an Internet-type network. The computer equipment 3 can be servers, workstations, etc.

[0068] In an intrinsically known way, the data 4 include transported data 7 that conform to at least one application protocol 8, as well as transport data 9 (see Fig. 2).

[0069] The access device 6 according to the invention includes an operating system 10. The operating system 10 includes appropriate analysis modules 14 for each application protocol used 8. The analysis modules 14 of the operating system 10 filter the transported data 7.

[0070] Each analysis module 14 implements a finite-state machine 11 representing a given application protocol 8. In order to create an analysis module 14, each finite-state machine 11 is modeled in the form of a model 12, particularly by using a state transition matrix. Next, the analysis module 14 for each application protocol 8 is generated, by means of an interpreter 13, from each model 12 (see Fig. 4).

[0071] Each analysis module 14 includes first information processing means 17 for verifying the conformity of the transported data with the application protocols 8 involved. Each analysis module 14 also includes second information processing means 18 for restricting the capabilities offered by an application protocol 8.

[0072] The operating system and the associated analysis modules 14 constitute means for filtering the transported data 7.

[0073] The access device 6 also comprises parameterization means 19. These parameterization means 19 allow a network administrator 15 to parameterize the analysis modules 14 in accordance with predetermined restrictions 16, as will be explained below.

[0074] As a result of the access device 6 according to the invention, it is possible to verify proper conformity with the application protocols, which makes it possible to block a very large number of "application" attacks without knowing what they are, including those that violate the RFCs ("IP standards"). Let's briefly recall that in the sense of the present invention, the abbreviation RFC (Request for Comment) designates various standard-setting documents in which the various protocols of the TCP/IP family are specified.

[0075] In addition, the technology according to the invention makes it possible to restrict the capabilities offered by an application. For example, the technology according to

the invention makes it possible to limit the commands available in an "application" protocol or to only authorize access to certain data, etc.

[0076] As a result of the combination of these two functionalities, (Verify and Restrict), the technology according to the invention makes it possible to detect and block a large number of "application" attacks. These two functionalities have been shown to detect and block 90% of the known attacks on Apache and IIS Web servers without its being necessary to integrate an "attack signature base" into them, as in the case of intrusion detection systems.

The technology according to the invention was developed on a Linux operating system. It is within the capability of one skilled in the art to implement it in other systems of the same type.

LIST OF TERMS

Term	Ref. Num.
Information	1
computing resources	2
group of computer equipment	3
Data	4
computer telecommunication network	5
access device	6
transported data	7
application protocol	8
transport data	9
operating system	10
finite-state machine	11
Model	12
Interpreter	13
analysis module	14
network administrator	15
predetermined restrictions	16
first information processing means	17
second information processing means	18
parameterization means	19